Amendment to the Claims:

This listing of claims will replace all versions, and listings, of claims in the application:

1. (Currently amended) A method of secure communication comprising:

establishing a secure tunnel between a server of an associated network and a peer using an encryption algorithm that establishes [[an]]a server encryption key possessed by the server and a peer encryption key possessed by the peer;

authenticating the peer with the server over the secured tunnel establishing [[an]]a server authentication key possessed by the server and a peer authentication key possessed by the peer;

hashing the server encryption key and the server authentication key to produce a first hash;

hashing the peer encryption key and the peer authentication key to produce a second hash;

verifying by the server that the peer possesses the same encryption and authentication keys as the server by comparing the first hash with the second hash;

~~provisioning~~distributing a network access credential from the server to the peer using the secured tunnel, responsive to the verifying the peer possesses the same encryption and authentication keys as the server; and

signaling an authorization failure to the peer ~~upon conclusion of~~in accordance with the ~~provisioning~~distributing of the network access credential, prior to the peer authenticating with the associated network using the ~~provisioned credentials~~distributed network access credential, and denying by the [[peer]]server access to the network by the [[server]]peer until the peer authenticates with the associated network using the ~~provisioned credentials~~distributed network access credential.

2. (Original) The method of claim 1 wherein the communication implementation between the at least first and second parties is at least one of a wired implementation and a wireless implementation.

3. (Original) The method of claim 1 wherein the encryption algorithm is an asymmetric encryption algorithm.

4. (Original) The method of claim 3 wherein the asymmetric encryption algorithm is used to derive a shared secret, subsequently used in the step of establishing a secure tunnel.

5. (Currently amended) The method of claim 3 wherein: the asymmetric encryption algorithm is Diffie-Hellman key exchange; and, the secure tunnel is a Diffie-Hellman tunnel.

6. (Previously presented) The method of claim 1 wherein the step of authenticating the peer is performed using Microsoft MS-CHAP v2.

7. (Original) The method of claim 1 further comprising a step of provisioning a public/private key pair on one of the at least first and second parties, and then to provision that public key on the respective remaining ones of the at least first and second parties.

8. (Original) The method of claim 7 wherein the step of provisioning a public/private key pair comprises providing a server-side certificate in accordance with Public Key Infrastructure (PKI).

9. (Currently amended) ~~An implementation~~A system for enabling secure communication between a peer and a server of an associated network, the system comprising:

~~an implementation~~means for establishing a secure tunnel between the server and the peer using an encryption algorithm that establishes [[an]]a server encryption key possessed by the server and a peer encryption key possessed by the peer;

~~an implementation~~means for authenticating the peer with [[a]]the server [[using]]by cryptography with [[an]]a server authentication key possessed by the server and a peer authentication key possessed by the peer;

~~an implementation~~means for hashing the server encryption key and the server authentication key to produce a first hash;

~~an implementation~~means for hashing the peer encryption key and the peer authentication key to produce a second hash;

~~an implementation~~means for verifying by the server that the peer possesses the same encryption and authentication keys as the server by comparing the first hash with the second hash;

~~an implementation~~means for ~~providing~~distributing a network access credential from the server to the peer via the secure tunnel responsive to successfully authenticating the peer and verifying by the server that the peer possesses the same encryption and authentication keys; and

~~an implementation~~means for signaling an authorization failure to the peer ~~upon conclusion of~~in accordance with the ~~provisioning~~distributing of the network access ~~credentials~~credential, prior to the peer authenticating with the associated network using the ~~provisioned credentials~~distributed network access credential, and denying by the [[peer]]server access to the network by the ~~server~~peer until the peer authenticates using the distributed network access credential.

10. (Currently amended) The ~~implementation~~system of claim 9 wherein the ~~implementation~~means for enabling communication between server and peer is at least one of a wired implementation and a wireless implementation.

11. (Currently amended) The ~~implementation~~system of claim 9 wherein the encryption algorithm is an asymmetric encryption algorithm.

12. (Currently amended) The ~~implementation~~system of claim 11 wherein the asymmetric encryption algorithm is used to derive a shared secret, subsequently used in the step of establishing a secure tunnel.

13. (Currently amended) The ~~implementation~~system of claim 11 wherein the asymmetric encryption algorithm is Diffie-Hellman key exchange.

14. (Original) The implementation of claim 9 wherein the implementation for authenticating comprises Microsoft MS-CHAP v2.

15. (Currently amended) The ~~implementation~~system of claim 9 further comprising ~~an implementation~~means for provisioning a public/private key pair on one of the at least server

and peer, and then to provision that public key on the respective remaining ones of the at least server and peer.

16. (Currently amended) The ~~implementation~~system of claim 15 wherein the ~~implementation~~means for provisioning a public/private key pair comprises ~~and~~ ~~implementation~~means for providing a server-side certificate in accordance with Public Key Infrastructure (PKI).

Claims 17 - 27 (Canceled)

28. (Currently amended) The method of claim 1, further comprising invalidating a secure credential for the peer responsive to a failure of one of the group consisting of: the establishing the secure tunnel between the server and the peer, ~~authentication~~the authenticating the peer with the server over the secure tunnel, and the verifying that the peer has the same encryption and authentication keys as the server.

29. (Currently amended) The method of claim 5, further comprising:
detecting a man-in-the-middle attack over the ~~Diffie-Helman~~Diffie-Hellman tunnel; and
selecting an alternate asymmetric encryption algorithm responsive to detecting the attack.

30. (Currently amended) The method of claim 5, wherein the ~~Diffie-Helman~~Diffie-Hellman key exchange is one of server-authenticated or anonymous.

31. (New) The method of claim 1, further including:
during the authorizing, monitoring access to the server over the secured tunnel; and,
determining an attack tunneling in accordance with the monitoring.

32. (New) The system of claim 9 further including:

means for monitoring, during the authorizing, access to the server over the secured tunnel; and,

means for determining an attack tunneling in accordance with a signal from the means for monitoring.